splunk>

FACT SHEET

Splunk® App for Active Directory

Real-time Monitoring and Auditing for Microsoft Windows Server Active Directory

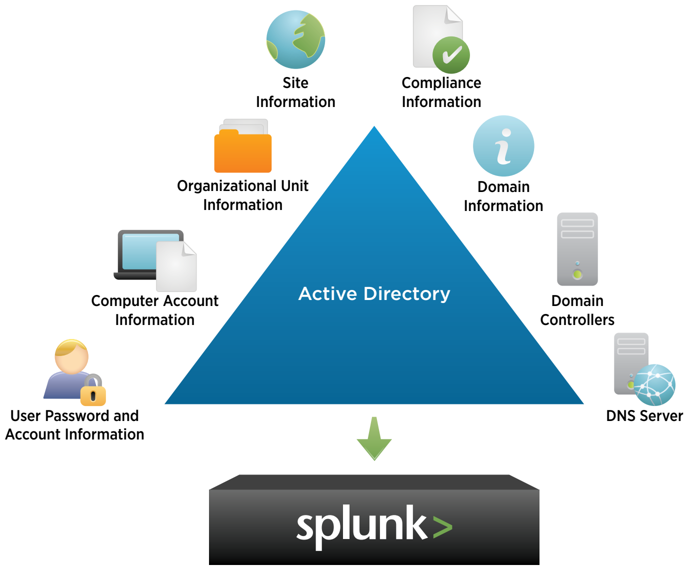
HIGHLIGHTS

- Real-time operational health and performance data of the Windows Server Active Directory Infrastructure
- Integrated auditing features that track activity from root domains to the individual objects in a site
- Extensive change management reports that deliver views to changes in objects and policies templates, increasing uptime

Microsoft Windows Server Active Directory is the foundation of an IT infrastructure. It is the central location for user configuration information, authentication requests and information about all the computers that run your business. When issues occur in Active Directory, the effect is evident and widespread—users are unable to login, access privileges expire, e-mail stops flowing and websites hang, Organizations need a proactive, easy-to-deploy solution that will uncover the data needed to diagnose the issue, fix its root cause and restore service.

Splunk App for Active Directory

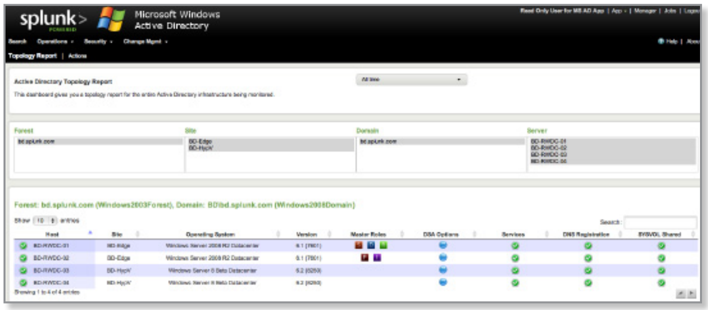
The Splunk App for Active Directory was designed to tackle the challenges faced by IT organizations—avoiding service outages, as well as proactive management and compliance reporting of the Active Directory infrastructure—from one place. This allows administrators to avoid the problems of traditional tools that just deliver health statistics, but miss reporting crucial compliance and auditing information. By monitoring the health and performance of an Active Directory Forest—from the forest, domains and sites that comprise the structure to the individual objects that represent tangible assets and then adding on compliance and auditing information—administrators can gain real-time operational intelligence about the entire Active Directory infrastructure. Armed with this deep insight from the data that is captured from Security, System and Audit logs, performance monitors and active service monitoring, your Active Directory Administrator can quickly pinpoint problems, identify security breaches and ensure corporate compliance goals.



Active Directory Data Inputs

With the Splunk App for Active Directory you can:

- Monitor Active Directory Forest for potential security breaches and non-compliant usage patterns
- Audit changes to group policies, user, group and computer objects in real time
- View detailed topology statistics on all the objects of your Active Directory top down from the Forest to individual user and computer accounts
- Monitor the operational health of Active Directory across site and domain boundaries


splunk> POWERED
Microsoft Windows Active Directory
Read Only User for MS AD App | App | Manager | Jobs | Logout
Search
Operations
Security
Change Mgmt
Help | About
Topology Report | Actions
All time

Active Directory Topology Report

This dashboard gives you a topology report for the entire Active Directory infrastructure being monitored.

Forest	Site	Domain	Server
bd.splunk.com	BD-Edge BD-HypV	bd.splunk.com	BD-RWDC-01 BD-RWDC-02 BD-RWDC-03 BD-RWDC-04

Forest: bd.splunk.com (Windows2003Forest), Domain: BD\bd.splunk.com (Windows2008Domain)

Show 10 entries

Search:

Host	Site	Operating System	Version	Master Roles	DSA Options	Services	DNS Registration	SYSVOL Shared
BD-RWDC-01	BD-Edge	Windows Server 2008 R2 Datacenter	6.1 (7601)	■ ■ ■	●	✓	✓	✓
BD-RWDC-02	BD-Edge	Windows Server 2008 R2 Datacenter	6.1 (7601)	■ ■	●	✓	✓	✓
BD-RWDC-03	BD-HypV	Windows Server 8 Beta Datacenter	6.2 (8250)		●	✓	✓	✓
BD-RWDC-04	BD-HypV	Windows Server 8 Beta Datacenter	6.2 (8250)		●	✓	✓	✓

Showing 1 to 4 of 4 entries

Active Directory Forest Topology Report

Splunk App for Active Directory Features

The Splunk App for Active Directory provides several specialized features to monitor Active Directory, including:

Topology Reports – Displays a complete view of the entire Active Directory Forest and the underlying Domains, Sites and Domain Controllers that are being monitored. This allows an Active Directory administrator to view the entire Forest from one single view rather then opening multiple consoles for information.

Domain Services – Displays information on the Domains, Sites and Domain controllers that belong to the Active Directory Forest. The information here delivers real-time statistics as to how the individual components are operating and how they are working together. Information gathered here is used to troubleshoot login issues, account for missing object information due to replication failures, and monitor performance of the directory service and domain controller load.

DNS Services – Displays information about the health, configuration, and performance of the DNS servers and DNS zones that host the Active Directory domains. Due to the dependency that Active Directory has on DNS, any changes made to DNS servers, performance issues or outages can create service disruptions on the Active Directory side. The information here allows Active Directory Administrators to view information about the DNS infrastructure that is usually administered by the networking team to see if issues in DNS are impacting the Active Directory Forest, producing faster resolution times.

User Logon Failures – Displays failed attempts by users to log onto a specific domain in the Active Directory Forest. Information here is used to protect the Active Forest from malicious unauthorized login activities. From one console, administrators can then view the multiple ways a security breach may be attempted across the entire Forest.

Anomalous Logons – Displays information on uncharacteristic usage patterns, such as a user logging in from multiple workstations. The information gathered here can be used to monitor for attempted security breaches across the Forest.

User Utilization – Displays the user and workstation load managed by Active Directory Forest. Information here is used for monitoring the load Domain Controllers are carrying and can then be used to justify hardware and software acquisitions.

Change Management – Displays changes made to objects in the Active Directory Forest. Helpdesk and admin staff can track changes made to computer accounts, domain accounts, organizational units and group policy objects to decrease support calls and pinpoint user issues.

Product Requirements

Supported Windows Server Versions

The Splunk App for Active Directory supports Active Directory Forests running on Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2 and Windows Server 2012.

Splunk Requirements

All instances of Splunk in a Splunk App for Active Directory requires Splunk Enterprise v4.3.2 or later and Sideview Utils v1.2.5 or later. All universal forwarders in a Splunk App for Active Directory deployment must run Splunk Enterprise v4.2.5 or later.

Free Download

Download Splunk. You'll get a Splunk Enterprise license for 60 days and you can index up to 500 megabytes of data per day. You can convert to a perpetual Free license or purchase an Enterprise license by contacting sales@splunk.com.

Try Out the App, it's Free!

Go to www.splunk.com/microsoft to learn more.